

Политика противодействия отмыванию денежных средств и финансированию террористической деятельности

1. Общие положения

- 1.1. Политика противодействия отмыванию денежных средств и финансированию террористической деятельности (далее Политика ОД/ФТ) является составной и неотъемлемой частью Клиентского соглашения.
- 1.2. Компания Fort Financial Services Ltd (далее Компания) неукоснительно соблюдает действующее международное законодательство в области противодействия легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма.
- 1.3. В рамках данной Политики ОД/ФТ в Компании утверждена Политика «Знай своего Клиента», выражающаяся в постоянном анализе и мониторинге Клиента Компании и его деятельности на торговых счетах.
- 1.4. В рамках данной Политики ОД/ФТ в Компании утверждена Политика Возврата денежных средств.
- 1.5. Основными целями Политики ОД/ФТ являются:
 - создание сбалансированных принципов Политики ОД/ФТ и разумное выполнение их таким образом, чтобы своевременно выявлять преступную деятельность Клиентов на своих торговых счетах, уменьшая при этом ее воздействие на законопослушных Клиентов;
 - обеспечение сохранности деловой репутации Компании;
 - исключение вовлечения и соучастия сотрудников Компании в процесс легализации доходов, полученных незаконным путем и финансирования терроризма.
- 1.6. Настоящая Политика ОД/ФТ устанавливает общие правила внутреннего контроля Клиентов и обязательна к исполнению всеми сотрудниками Компании.

2. Общие принципы Политики противодействия отмыванию денежных средств и финансированию террористической деятельности

- 2.1. Компания не осуществляет открытие торгового счета на анонимного владельца.
- 2.2. Компания имеет право заблокировать вход в Личный кабинет, приостановить торговую деятельность на счетах, либо отменить заявку на ввод/вывод денежных средств, если в процессе взаимодействия Клиента (для юридических лиц: владельцев или директоров) с Компанией появляются сведения об участии Клиента (представителей компании) в экстремистской деятельности или деятельности, связанной с отмыванием денежных средств .
- 2.3. Компания не принимает наличные деньги от Клиентов в качестве депозита и не выплачивает наличные деньги ни при каких обстоятельствах.
- 2.4. Каждый Клиент Компании должен использовать для зачисления/снятия денежных средств электронный кошелек, принадлежащий только ему. При этом имя держателя электронного кошелька должно полностью соответствовать имени, указанному при регистрации Клиента на сайте Компании.
- 2.5. Использование одних и тех же платежных реквизитов разными Клиентами Компании запрещено.
- 2.6. Каждый Клиент Компании обязан верифицировать платежные реквизиты своих электронных кошельков в Личном Кабинете, которые он намерен использовать для осуществления операций по вводу и выводу средств.
- 2.7. В случае возникновения сомнений в достоверности и актуальности полученных данных о платежных реквизитах Клиента, Компания в праве запросить снимок экрана компьютера (screen shot), на котором открыта Интернет-страница платежной системы с размещенными на ней сведениями о владельце данного электронного кошелька.
- 2.8. Денежные средства внутри Компании могут переводиться только между счетами Клиента, прошедшего процедуру верификации личных данных. Перевод денежных средств между счетами и/или лицевыми счетами, принадлежащими разным Клиентам Компании, запрещен.
- 2.9. Денежные средства могут быть выведены только тем же способом и на те же реквизиты, с которых осуществлялся их ввод, если иное не предусмотрено правилами Компании.
- 2.10. Компания проводит обязательную верификацию Клиентов согласно Клиентскому

соглашению и в соответствии с принципами Политики «Знай своего Клиента».

3. Предоставление сведений в Уполномоченный орган

- 3.1. При обнаружении подозрительной деятельности, осуществляемой Клиентом на своих торговых счетах, сотрудник Компании обязан уведомить об этом Комплаенс Менеджера и направить ему все необходимые документы.
- 3.2. Каждый сотрудник компании обязан сообщать о любых подозрительных предложениях Клиентов, даже если операция не была проведена, Комплаенс Менеджеру.
- 3.3. Все действия, предпринятые в связи с операциями, сообщения о которых подлежат предоставлению в уполномоченный орган, подлежат документированию и хранятся с соблюдением установленных требований по обеспечению сохранности конфиденциальной информации.
- 3.4. Детали операций, сведения о которых подлежат предоставлению в уполномоченный орган, и любые контакты с уполномоченными органами в отношении этих операций документируются.

4. Конфиденциальность

- 4.1. Информация о Клиентах и их операциях, полученная в рамках принципов Политики ОД/ФТ, является конфиденциальной.
- 4.2. Сотрудники Компании и Комплаенс Менеджер не вправе информировать Клиентов и иных лиц о формах, способах и методах осуществления принципов Политики ОД/ФТ.
- 4.3. Раскрытие иным лицам информации о том, что Компанией были представлены в уполномоченный орган сведения об операциях или деятельности Клиента, строго запрещается.

5. Хранение документов и информации

- 5.1. Данные, полученные в результате идентификации Клиентов, и сведения об операциях хранятся как доказательство предпринятых Компанией в соответствии с действующей Политикой ОД/ФТ мер, а также для их использования в качестве доказательств при

проведении расследования уполномоченными органами.

- 5.2. Идентификационные данные Клиентов подлежат хранению в течение не менее пяти лет после прекращения отношений с Клиентом в соответствии с действующей Политикой «Знай своего Клиента».
- 5.3. Данные об операциях, сведения по которым были направлены в уполномоченный орган, подлежат хранению в течение не менее пяти лет с даты совершения операции.
- 5.4. Все внутренние и внешние отчеты, полученные в рамках реализации принципов Политики ОД/ФТ, подлежат хранению в течение не менее пяти лет с даты представления отчета.
- 5.5. Компании обязана хранить информацию обо всех действиях, предпринятых в связи с выполнением требований о получении от работников и представлении в уполномоченный орган сведений о выявленных операциях. В том случае, если принято решение не направлять в уполномоченный орган сведения относительно возможного отмывания денежных средств/финансирования терроризма, информация о данных фактах все равно подлежит хранению.